I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on November 3, 2009

TOWNSEND and TOWNSEND and CREW LLP

By: /Bonnie Ricklet/
Bonnie Ricklet

PATENT
Attorney Docket No. 026595-006400US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Robert Degen, et al.

Application No.: 10/091,000

Filed: March 4, 2002

For: MONEY TRANSFER EVALUATION SYSTEMS AND METHODS

Confirmation No. 6763

Examiner: Cristina O. Sherr

Technology Center/Art Unit: 3685

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF UNDER 37 CFR §41.37

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

Further to the Notice of Non-Compliant Appeal Brief mailed on October 9, 2009, for the above-referenced application, Appellants submit this Amended Brief on Appeal.

5. Summary Of Claimed Subject Matter

In the following summary, the Appellants have provided exemplary references to sections of the specification and drawings supporting the subject matter defined in the claims as required by 37 C.F.R. § 41.37. The specification and drawings also include additional support for other exemplary embodiments encompassed by the claimed subject matter. Thus, it should be appreciated that the references are intended to be illustrative in nature only.

The invention generally relates to technology for evaluating value transfers for suspect activities, such as, terrorist activities, money laundering, and the like. Application, page 2, lines 7-8. The various embodiments of the invention include receiving money transfers at a host computer system (Id. at page 2, lines 22-23; Figure 2; page 8, line 9 – page 9, line 24) and grouping money transfers into groups based on similarities between sender identification and receiver identification. Id. at page 2, lines 15-16. Money transfers within groups are analyzed for suspect activity. Id. at page 2, lines 25-27.

The embodiment of claim 1 relates to a method for evaluating electronic value transfers. Id. at page 2, lines 6-7, and FIGS. 7A and 7B. According to this embodiment, a plurality of money transfer requests are received at a host computer system. Id. at page 2, lines 22-23; Figure 2; page 8, line 9 – page 9, line 24. The money transfer requests include a first money transfer request and a second money transfer request. Id. at page 2, lines 13-17. The first money transfer request is associated with a first sender identification and the second money transfer request is associated with a second sender identification. Id. Records of the money transfer requests are electronically stored at a host computer system. Id. at page 2, line 23; Figure 2; page 8, line 9 – page 9, line 24. An analysis is performed on the records that indicates whether the first sender identification and the second sender identification are related at a host computer system. Id. at page 2, lines 23-25; Figure 2; page 8, line 9 – page 9, line 24. A reference designator is created at a host computer system. Id. at page 2, line 15, and Figs. 5, 6 and 8. The reference designator is associated with the first sender identification and the second

sender identification. Id. at page 2, lines 15-16. The reference designator is stored apart from the records of the money transfer requests. Id. at page 13, line 56, through page 14, line 3. The records of the money transfer requests are searched according to a specified criteria to determine if any of the money transfer requests associated with the reference designator are suspicious money transfer requests. Id. at page 2, lines 26-28. Suspicious money transfer requests are flagged at a host computer system. Id. at page 2, lines 28-29; Figure 2; page 8, line 9 – page 9, line 24. The first sender identification may include a sender name, a sender number, an agent number, a sending data, a sending location, a sender phone number, a sending time, a sending message, or a sending amount. Id. at page 10, lines 20-32. The suspicious money transfer requests are selected from the following: (a) a transfer from a first sender to a second sender followed within a specified period by a transfer from the second sender to the first sender (Id. at page 2, lines 31-33); (b) a group of transfers from a sender to a group of receivers, wherein the aggregate amount of the group of transfers exceeds a specified level (Id. at page 2, lines 33-34); (c) one or more transfers from a sender to a receiver, wherein the aggregate amount of the one or more transfers exceeds a specified level (Id. at page 2, line 34, through page 3, line 2); (d) a group of transfers from a group of senders to a receiver, wherein the aggregate amount of the group of transfers exceeds a specified level (Id. at page 3, lines 2-3); (e) two transfers from a first sender to a second sender that are followed within a specified period by corresponding transfers from the second sender to a receiver (Id. at page 3, lines 3-5); (f) two or more transfers from a sender to a receiver, wherein the two or more transfers are initiated from two or more distinct locations within a region (Id. at page 3, lines 5-7); and (g) two or more transfers from a sender to a receiver, wherein the two or more transfers are received at two or more distinct locations within a region (Id. at page 3, lines 7-9).

The embodiment of claim 16 relates to a method for evaluating electronic value transfers. Id. at page 2, lines 6-7, page 3, lines 10-11, and FIGS. 7A and 7B. According to this embodiment, a money transfer record is accessed at a fraud processing computer. Id. at page 2, lines 9-11, page 3, line 11; Figure 2; page 8, line 9 – page 9, line 24. The money transfer record includes a sender identification and a receiver identification. Id. at page 2, lines 23-25. A master

location identifier is assigned to the money transfer record at a fraud processing computer. Id. at page 3, lines 11-12; Figure 2; page 8, line 9 – page 9, line 24. The master location identifier is determined by one or both of the sender identification and the receiver identification. Id. at page 16, lines 7-10. The money transfer record is compared to a reference designator using a specified criteria at a fraud processing computer. Id. at page 3, lines 12-13; Figure 2; page 8, line 9 – page 9, line 24. A relationship between the reference designator and the money transfer record is indicated by one or more fields of the reference designator or the money transfer record. Id. at page 3, lines 13-15. The money transfer record is associated with the reference designator at a fraud processing computer. Id. at page 3, lines 15-16; Figure 2; page 8, line 9 – page 9, line 24.

The embodiment of claim 17 relates to a method for iteratively compiling suspicious money transfer activities from money transfer records. Id. at page 3, lines 17-18. According to this embodiment, a first money transfer record is accessed at a fraud processing computer (Id. at page 3, line 19; Figure 2; page 8, line 9 – page 9, line 24) and a first reference designator is provided at the fraud processing computer (Id. at page 3, line 19; Figure 2; page 8, line 9 – page 9, line 24). This first reference designator is associated with one or more of a sender identification and a receiver identification from a second money transfer record. Id. at page 2, lines 13-17. The first money transfer record is compared to the first reference designator using a specified criteria. Id. at page 3, lines 20-21. The comparison indicates the first money transfer record is not related to the first reference designator at the fraud processing computer. Id. at page 3, lines 21-22; Figure 2; page 8, line 9 – page 9, line 24. A second reference designator is created at the fraud processing computer that is associated with one or more of a sender identification and a receiver identification from the first money transfer record. Id. at page 3, lines 22-23; Figure 2; page 8, line 9 – page 9, line 24. The first and second reference designators are maintained in a reference designator list apart from the first and second money transfer records, reducing the performance impact upon a money transfer system under evaluation. Id. at page 23, lines 11-15. The reference designator list is analyzed for suspicious money transfer activities at the fraud processing computer. Id. at page 6, lines 6-8; Figure 2;

page 8, line 9 – page 9, line 24. The suspicious money transfer requests are selected from the following: (a) a transfer from a first sender to a second sender followed within a specified period by a transfer from the second sender to the first sender (Id. at page 2, lines 31-33); (b) a group of transfers from a sender to a group of receivers, wherein the aggregate amount of the group of transfers exceeds a specified level (Id. at page 2, lines 33-34); (c) one or more transfers from a sender to a receiver, wherein the aggregate amount of the one or more transfers exceeds a specified level (Id. at page 2, line 34, through page 3, line 2); (d) a group of transfers from a group of senders to a receiver, wherein the aggregate amount of the group of transfers exceeds a specified level (Id. at page 3, lines 2-3); (e) two transfers from a first sender to a second sender that are followed within a specified period by corresponding transfers from the second sender to a receiver (Id. at page 3, lines 3-5); (f) two or more transfers from a sender to a receiver, wherein the two or more transfers are initiated from two or more distinct locations within a region (Id. at page 3, lines 5-7); and (g) two or more transfers from a sender to a receiver, wherein the two or more transfers are received at two or more distinct locations within a region (Id. at page 3, lines 7-9).

The embodiment of claim 23 relates to a method for evaluating electronic value transfers. Id. at page 2, lines 6-7, and FIGS. 7A and 7B. According to this embodiment, money transfer requests are received at a computer (Id. at page 2, lines 22-23; Figure 2; page 8, line 9 – page 9, line 24) that include a user identification associated with each of the money transfer requests. Id. at page 2, lines 13-17. The money transfer requests have also been grouped based on similarities between the user identifications. Records of the money transfer requests are electronically stored at the computer. Id. at page 2, line 23; Figure 2; page 8, line 9 – page 9, line 24. The records of the money transfer requests are provided to a fraud processing computer. Id. at page 2, lines 12-13. An indication of a suspicious money transfer request is received at the computer that includes the user identification associated with the suspicious money transfer request. Id. at page 2, lines 26-29, and page 5, lines 25-29; Figure 2; page 8, line 9 – page 9, line 24. The suspicious money transfer requests are selected from the following: (a) a transfer from a first sender to a second sender followed within a specified period by a transfer from the second

sender to the first sender (Id. at page 2, lines 31-33); (b) a group of transfers from a sender to a group of receivers, wherein the aggregate amount of the group of transfers exceeds a specified level (Id. at page 2, lines 33-34); (c) one or more transfers from a sender to a receiver, wherein the aggregate amount of the one or more transfers exceeds a specified level (Id. at page 2, line 34, through page 3, line 2); (d) a group of transfers from a group of senders to a receiver, wherein the aggregate amount of the group of transfers exceeds a specified level (Id. at page 3, lines 2-3); (e) two transfers from a first sender to a second sender that are followed within a specified period by corresponding transfers from the second sender to a receiver (Id. at page 3, lines 3-5); (f) two or more transfers from a sender to a receiver, wherein the two or more transfers are initiated from two or more distinct locations within a region (Id. at page 3, lines 5-7); and (g) two or more transfers from a sender to a receiver, wherein the two or more transfers are received at two or more distinct locations within a region (Id. at page 3, lines 7-9).

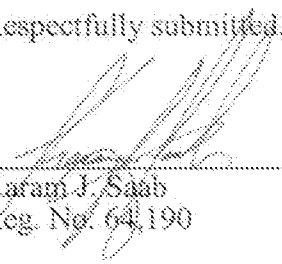
The embodiment of claim 24 relates to a system for evaluating value transfers. Id. at page 2, lines 6-7, and FIGS. 7A and 7B. The system includes a fraud processing computer and a computer readable medium associated with the fraud processing computer. Id. at page 2, lines 12-13. The computer readable medium includes computer instructions executable by the fraud processing computer to access a first money transfer record. Id. at page 2, lines 13-15. The computer readable medium also includes computer instructions executable by the fraud processing computer to provide a first reference designator. Id. at page 2, lines 15-16. The first reference designator is associated with one or more of a sender identification and a receiver identification from a second money transfer record. Id. The computer readable medium also includes computer instructions executable by the fraud processing computer to compare the first money transfer record to the first reference designator using a specified criteria. Id. at page 2, lines 16-17 and 26-28. The comparison indicates that the first money transfer record is not related to the first reference designator. Id. at page 2, lines 17-18, and page 3, lines 21-23. The computer readable medium also includes computer instructions executable by the fraud processing computer to create a second reference designator. Id. at page 2, lines 18-20. The first reference designator is associated with one or more of a sender identification and a receiver

identification from the first money transfer record. Id. at page 3, lines 22-23. The first and second reference designators are maintained in a reference designator list apart from the first and second money transfer records, wherein a performance impact of the method upon a money transfer system under evaluation is reduced. Id. at page 23, lines 11-15.

The embodiment of claim 27 relates to a system for transferring value. Application, page 6, lines 4-6. The system includes a money transfer system. Id., at page 2, lines 16, 17. The system also includes a fraud processing server communicably coupled to the money transfer system. Id. The money transfer records associated with the money transfer system are accessible by the fraud processing server in order to cluster related money transfer records separately from the money transfer records associated with the money transfer system in order to use the clustered records to identify any suspicious money transfer requests. Id., at page 2, lines 17-20. The suspicious money transfer requests are selected from a group consisting of: (a) a transfer from a first sender to a second sender followed within a specified period by a transfer from the second sender to the first sender (Id., at page 2, line 30 – page 3, line 9);(b) a group of transfers from a sender to a group of receivers, wherein the aggregate amount of the group of transfers exceeds a specified level (Id., at page 2, line 30 – page 3, line 9); (c) one or more transfers from a sender to a receiver, wherein the aggregate amount of the one or more transfers exceeds a specified level (Id., at page 2, line 30 – page 3, line 9); (d) a group of transfers from a group of senders to a receiver, wherein the aggregate amount of the group of transfers exceeds a specified level (Id., at page 2, line 30 – page 3, line 9); (e) two transfers from a first sender to a second sender that are followed within a specified period by corresponding transfers from the second sender to a receiver (Id., at page 2, line 30 – page 3, line 9); (f) two or more transfers from a sender to a receiver, wherein the two or more transfers are initiated from two or more distinct locations within a region (Id., at page 2, line 30 – page 3, line 9); and (g)

two or more transfers from a sender to a receiver, wherein the two or more transfers are received at two or more distinct locations within a region (Id., at page 2, line 30 – page 3, line 9).

Respectfully submitted,



Karam J. Saab
Reg. No. 64,190

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 303-571-4321

62289160 v1